Amendments & Clarification - Ref: CO:ITD:25/R1:2019-20 dated 10.04.2019 for "Procurement of DLP (Data Leak Prevention) Solution with required hardware / software at Data Centre (Chennai) and DR Site (Hyderabad) with 1 year warranty and 4 years support"

Amendments:

S.no.	References	Existing Clause	Queries / Change Requested	Amended Clause	Reason
1	Page no. 14 Clause no 4.2	Implementation of the solution has to be done within 3 months from the date of purchase order.	Requested as 8 months. Requested as 6 months. Requested as 6 months.	Implementation of the solution has to be done within 4 months from the date of purchase order.	Data classification has to be done by the bidder, so one month extra time is being provided.
2	Page no. 23 Section IV	Bank reserves its right to decide whether or not to enter into renewal for the DLP solution after the initial lock in period of 1 (One) year.	DLP Solution Implementation and management is a long-term project and typically all the banks and financial institutions have gone for 5 years contract to realize the benefits of the implemented solution. We request the bank to confirm the contract period for five years.	Bank reserves its right to decide whether or not to enter into renewal for the DLP solution after the contract period of 5 (Five) years.	The Clause stands corrected as 5 years instead of 1 year.
3	Page no. 24 Clause no. 6	The Proposed Solution should capture logs of Data Transfer through any medium like E-Mail, Internet Upload, USB Transfer etc. At the same time intelligently co-relate and analyses these Logs with previous user based attempts / incidents and trigger alerts.	This is a functionality of SIEM to correlate the incidents. The primary role of DLP is to trigger the policy violation based on the parameters that are configured in the policy. Since it is not a functionality of DLP, hence requesting M/s. Indian Bank to consider removing this point.	The Proposed Solution should capture logs of Data Transfer through any medium like Internet Upload, USB Transfer etc. At the same time intelligently co-relate and analyses these Logs with previous user based attempts / incidents and trigger alerts.	Capturing logs from E-mail has been removed due to Mail DLP is not required.
4	Page no. 24 Clause no. 12	Ability to integrate with threat intelligence for enterprises across all locations.	DLP is a solution for data loss; DLP solution will not cover threat intelligence. Threat intelligence comes with the security solutions.	Specification stands deleted.	Since all the bidders have informed that threat intelligence is not forming part of DLP solution, the clause stands deleted.
5	Page no. 24 Clause no. 13	The Solution should have a capability to capture and index all the traffic flowing out of the	The proposed solution is a DLP technology which captures all contents instead of traffic flow. Hence request to modify this	The Solution should have a capability to capture, index and store all the traffic which	Bank needs to inspect only that traffic which violated the policy.

		Network.	specification as " The solution should have capability to detect the data breach and store the incident for forensic purpose"	violated the policy.	
6	Page no. 25 Clause no. 15	The proposed solution should have the capability to analyse: • file formats (.doc, .docx, .xls,.xlsx,.ppt,.pptx, .csv, .pdf, .xps etc) • data in archival tools (.zip/.rar/.7z/.tar) • encrypted data over web proxies • data sent over email • attachments of the email	Email attachments can only be Monitored & protected when we will have the Mail DLP component.	The proposed solution should have the capability to analyse: • file formats (.doc, .docx,.xls,.xlsx,.ppt,.pptx, .csv, .pdf, .xps etc) • data in archival tools(.zip/.rar/.7z/.tar) • encrypted data over web proxies	Data sent over e-mail has been removed from the specification.
7	Page no. 25 Clause no. 23	The proposed solution should generate (exception) alerts and reports for contents that could not be decrypted for analysis as part of DLP solution.	We need clarify on this specification as we detect the encrypted files and alert the admins. Also we request M/s. Indian Bank to modify the specification as " The proposed solution should be able to detect the encrypted files and trigger incidents" Please elaborate	The proposed solution should be able to detect the encrypted files and trigger incidents. The proposed solution should generate (exception) alerts and reports for contents that could not be decrypted for analysis as part of DLP solution.	Improvement in the specification has been done after the change.
8	Page no. 25 Clause no. 34	The Proposed Solution should be able to perform following Searches: • E-Mail Sent from or to any E-Mail Address.	Need more clarity on what is expected in the search. This is a DLP solution which generates incidents based on content and captures required fields. Email attachments can only be Monitored & protected when we will have the Mail DLP component.	Specification stands deleted.	Mail DLP is not a part of the solution.
9	Page no. 26 Clause no. 41	The solution should have ability to detect cumulative malware information leaks. The solution should be able to detect data leaks	DLP is a solution for data loss; DLP solution will not cover malware information leaks. Detecting data leaks over to competitors and the data sent and uploaded after the office	The solution should be able to detect data leaks over to competitors and the data sent and uploaded after the office	Malware information leak is removed as it does not come in scope of DLP.

		over to competitors and the data sent and uploaded after the office hours predefined patterns. The solution should also be capable of detecting and blocking the sensitive information uploads to Group of P2P software i.e. Bit Torrent, eMule etc.	hours predefined patterns will not be covered with data loss as it depends on the User Behaviour. Not a data loss prevention use cases, it will be a proxy based solution.	hours predefined patterns. The solution should also be capable of detecting and blocking the sensitive information uploads to Group of P2P software i.e. Bit Torrent, eMule etc.	
10	Page no. 27 Clause no. 52	The solution must manage all DLP security products (e.g., software, appliances) from one centralized administration console, even encryption of files and folders.	This is DLP specification. The file and folder encryption is a different technology, hence requesting M/s. Indian Bank to remove this point.	The solution must manage all DLP security products (e.g., software, appliances) from one centralized administration console.	File and folder encryption does not come under the scope of DLP.
11	Page no. 27 Clause no 60	The solution should be able to detect sensitive data going out in the form of all different images formats.	Both are same points, so kindly requesting M/s. Indian Bank to remove any one of the above specifications.	Clause stands deleted.	This specification is already covered in clause no. 64

Clarifications:

S.no.	References	Existing Clause	Queries / Changes Requested	Clarification from Bank
1	Page no. 8 Clause no. 6	6.1 The bidder shall furnish, as part of their bid, a bid security in the form of a bank guarantee issued by a scheduled commercial bank or foreign bank located in India, in the form provided in the bidding documents for a sum of (Rupees Thirty lakhs only) and valid for forty five days (45) days after the validity of the bid (i.e. Bid validity 120 days + 45 days = 165 days from the last date for submission of bid). Bank may seek extension of Bank Guarantee, if required. 6.2 Unsuccessful Bidders' bid security will be discharged or returned after completion of purchase process. 6.3 The successful bidder's bid security will be discharged upon the bidders signing the contract and furnishing the performance security.	6.1 The bidder shall furnish, as part of their bid, a bid security in the form of a bank guarantee issued by a scheduled commercial bank or foreign bank located in India, in the form provided in the bidding documents for a sum of (Rupees Thirty lakhs only) and valid for forty five days (45) days after the validity of the bid (i.e. Bid validity 90 days~~120 days~~ + 30 days~~45 days~~ = ~~165~~ 120 days from the last date for submission of bid). Bank may seek extension of Bank Guarantee, if required. 6.2 Unsuccessful Bidders' bid security will be discharged or returned ~~after completion of purchase process~~. On rejection of Bid 6.3 The successful bidder's bid security will be discharged upon the bidders signing the contract and furnishing the performance security.	Please adhere to RFP terms and conditions.
2	Page no. 8 Clause no. 6	With the requirement of signing of contract and Failure of the successful Bidder to comply performance Security shall constitute sufficient grounds for annulment of the award and forfeiture of the bid security, in which event the Bank may call for new bids.	With the requirement of signing of contract and Failure of the successful Bidder to comply performance Security shall constitute sufficient grounds for annulment of the award and ~~forfeiture of the bid security,~~ in which event the Bank may call for new bids.	Please adhere to RFP terms and conditions.
3	Page no. 8 Clause no. 7	Bids shall remain valid for the period of 120 days after the last date for submission of bid prescribed. A bid valid for a shorter period shall be rejected by the bank as non-responsive. Bank may seek extension of bid validity, if required.	Bids shall remain valid for the period of ~~120~~ 90 days after the last date for submission of bid prescribed. A bid valid for a shorter period shall be rejected by the bank as non-responsive. Bank may seek extension of bid validity, if required.	Please adhere to RFP terms and conditions.
4	Page no. 14 Clause no 4.2	Implementation of the solution has to be done within 3 months from the date of purchase order.	Requested as 8 months. Requested as 6 months. Requested as 6 months.	Please refer to amendment no. 1
5	Page no. 14 Clause no. 5.2	Payment Terms - 30% on BOM & POST,	Requested Payment Terms - 70% on BOM & POST verification,	Please adhere to the terms and conditions of RFP.

		40% on Installation & Configuration and Testing of 10 Clients on Web and Endpoint, 20% on Implementation closure including integration with existing devices and applications, also with and solutions procured in this RFP, making the device/solution operational (as per Purchaser's scope), UAT, and receiving sign off from the Purchaser & 10% on 3 months post sign off.	10% on Installation & Configuration and Testing of 10 Clients on Web and Endpoint, 10% on Implementation closure including integration with existing devices and applications, also with and solutions procured in this RFP, making the device/solution operational (as per Purchaser's scope), UAT, and receiving sign off from the Purchaser & 10% on 3 months post sign off.	
			90% on BOM & POST verification, 10% on 3 months post sign off.	
6	Page no. 14 Clause no. 5.2	Payment AMC/Software subscription, subsequent Payment will be made in every 6 months in arrears	We request AMC/Software subscription, subsequent Payment shall be made yearly Advance. We request AMC/Software subscription, subsequent Payment shall be made yearly Advance.	Please adhere to RFP terms and conditions.
7	Page no. 14 Clause no. 5.3	Prices payable to the Supplier as stated in the Contract shall be firm and not subject to adjustment during performance of the Contract.	Prices payable to the Supplier as stated in the Contract shall be firm and not subject to adjustment during performance of the Contract. In the event the Base Exchange Rate either increases or decreases by percentage points greater than two per cent [2%], the prices shall be charged as per the then current exchange rate Any increase or decrease in the rates of the applicable taxes, duties or any new levy on account of changes in law shall be to the account of Customer.	Please adhere to RFP terms and conditions.
8	Page no. 14 Clause no. 6	The Bank will consider the inability of the vendor to deliver or install the equipment within the specified time limit, as a breach of contract and would entail the payment of Liquidation Damages on the part of the vendor. Notwithstanding the Purchaser's right to cancel the order, Liquidated Damages at 0.5% of the invoice price of the solution/services will be charged for every week's delay in the delivery/installation and implementation of the	Please confirm that Liquidated Damages will be calculated only on the undelivered equipment value not on the total invoice value.	Please adhere to RFP terms and conditions.
			This penalty clause for Delivery & Implementation will NOT be applicable to the System Integrator for the Reasons attributable by the BANK.	It is clarified that the LD for delivery and implementation will not be applicable for reasons attributable by the BANK.

		solution beyond the specified delivery/commission period of each solution subject to a maximum of 10% of the total contract value of that solution/service.		However the successful bidder should inform the Bank that the delivery and implementation timelines could not be met due to reason listed and the same being accepted by the Bank.
9	Page no. 15 Clause no. 7	The supplier undertakes that warranty support of 1 year shall start after the Solutions with software and hardware have been installed at the final destination indicated in the contract and from the date of sign off of the respective solutions.	We request that warranty for one year shall commence either from the date of installation or on completion of 90 days from date of delivery, whichever is earlier.	Please adhere to RFP terms and conditions.
10	Page no. 15 Clause no. 7	The Supplier warrants, for the duration of the Warranty Period commencing from the date of implementation at all sites, that all the deliverables supplied under this Contract shall have no critical defect arising from design or from any act or omission of the Supplier that may develop under normal use of the deliverables.	The Supplier warrants, for the duration of the Warranty Period commencing from the date of ~~implementation~~ delivery at all sites, that all the deliverables supplied under this Contract shall have no critical defect arising from design or from any act or omission of the Supplier that may develop under normal use of the deliverables.	Please adhere to RFP terms and conditions.
11	Page no. 17 Clause no. 9	The operation hours are defined as 24 X 7 X 365.	Does Bank allow Shared Remote SOC service for 24X7X365 coverage?	Bank's SOC Team is available 24 x 7 x 365.
12	Page no. 17 Clause no. 9	SLA Table	Is there possibility of relaxing Penalty and non-adherence to SLAs for 1%, 2%, 3%, 5% at the max.? Currently it seems pretty high at (1%, 3%, 5% and 10% of subscription and licence for 1 year).	Please adhere to RFP terms and conditions.
		Penalty on non-adherence to SLAs.	This penalty clause for SLA will not be applicable to the System Integrator for the Reasons attributable by the BANK.	Accepted. However the successful bidder should inform the Bank that the SLA could not be met due to reason listed and the same being accepted by the Bank.
13	Page no. 18 Clause no. 9	If a breech occurs due to failure of DLP solution, a Penalty of Rs.1000/- per event will be deducted.	Request to change the penalty to Rs.250/- Per event.	Please adhere to terms and conditions of RFP.

14	Page no. 18 Clause no. 9	If a Breach occurs due to failure of DLP Solution, a penalty of 1000 per event will be detected.	Please share the detailed definition of DLP event to on-board and accommodate the same from Solution proposal prospective.	It is clarified that if any Data is leaked to users other than permitted users as per DLP policy, due to the failure of DLP solution (i.e. DLP solution has not prevented the leakage) will be known as DLP event.
15	Page no. 18 Clause no. 9	The right to levy the penalty is in addition to and without prejudice to other rights / remedies available to the Bank such as termination of contract, invoking performance guarantee and recovery of amount paid etc.	The right to levy the penalty is in addition to and without prejudice to other rights / remedies available to the Bank such as termination of contract after payment for goods and services rendered ,~~invoking performance guarantee and recovery of amount paid etc.~~ The aggregate penalty that can be deducted in a month shall be restricted to a maximum of 3% of the service charges payable to Service Provider for that month.	Please adhere to RFP terms and conditions.
16	Page no. 19 Clause no. 15	The Bank, by 30 days written notice sent to the successful bidder, may terminate the Contract, in whole or in part, at any time for its convenience. The notice of termination shall specify that termination is for the Bank's convenience, the extent to which performance of the successful bidder under the Contract is terminated, and the date upon which such termination becomes effective.	~~The Bank~~,Either Party by ~~30~~ 90 days written notice sent to the successful bidder, may terminate the Contract, in whole or in part, at any time for its convenience. The notice of termination shall specify that termination is for the Bank's convenience, the extent to which performance of the successful bidder under the Contract is terminated, and the date upon which such termination becomes effective. In the event of termination the Contractor shall be paid for the: a) Goods delivered b) Services rendered c) Work in progress d) Third party orders in pipeline which cannot be cancelled despite Contractor's best efforts e) Unrecovered investments shall be paid by customer as per termination schedule till the date of termination.	Please adhere to RFP terms and conditions.
17	Page no. 19 Clause no. 16	The Bank, without prejudice to any other remedy for breach of contract, by 15 days written notice of	We request to remove this clause. The Bank, without prejudice to any other remedy for breach of contract, by ~~15~~ 30 days written notice of	Please adhere to RFP terms and conditions.

		default sent to the Successful bidder, may terminate this Contract in whole or in part In the event the Bank terminates the Contract in whole or in part, the Bank may procure, upon such terms and in such manner as it deems appropriate, Goods or Services similar to those undelivered, and the Successful bidder shall be liable to the Bank for any excess costs for such similar Goods or Services. However, the successful bidder shall continue performance of the Contract to the extent not terminated.	default sent to the Successful bidder, may terminate this Contract in whole or in part In the event of termination Customer shall pay Bidder for goods delivered and services rendered till the date of termination. In the event the Bank terminates the Contract in whole or in part, the Bank may procure, upon such terms and in such manner as it deems appropriate, Goods or Services similar to those undelivered, and the Successful bidder shall be liable to the Bank for any excess costs for such similar Goods or Services. Provided further that the Vendor shall not be liable to Excess Cost in excess of (ten) 10 percent of the price of undelivered goods or services for which such option is exercised by the Purchaser. However, the successful bidder shall continue performance of the Contract to the extent not terminated.	
18	Page no. 21 Clause no. 23	The Purchaser acknowledges that no promise, representation, warranty or undertaking has been or will be made or given by the Successful bidder or any person on behalf of the Successful bidder in relation to the Support Services, the Systems or this Agreement including the quality of the support Services or any goods supplied. The Purchaser has relied upon its own skill and judgment in opting for these services. Save where herein expressly provided, all whatsoever other warranties implied by law are hereby excluded,	The Purchaser acknowledges that no promise, representation, warranty or undertaking has been or will be made or given by the Successful bidder or any person on behalf of the Successful bidder in relation to the Support Services, the Systems or this Agreement including the quality of the support Services or any goods supplied. The Purchaser has relied upon its own skill and judgment in opting for these services. Save where herein expressly provided, all whatsoever other warranties implied by law are hereby excluded, Notwithstanding anything contained herein, neither Party shall be liable for any indirect, punitive, consequential or incidental loss, damage, claims, liabilities, charges, costs, expense or injury (including, without limitation, loss of use, data, revenue, profits, business and for any claims of any third party claiming through Wipro) that may arise out of or result from this Agreement. The aggregate liability of Wipro, under this Agreement, shall not exceed the fees (excluding	Please adhere to RFP terms and conditions.

			reimbursements) received by it under this contract during the six months preceding the date of first claim.	
19	Page no. 22 Clause no. 26	As per the scope of the RFP, subcontracting is prohibited.	Please confirm whether the subcontracting is allowed or not.	Please adhere to terms and conditions of RFP.
20	Page no. 23 Section IV	Bank reserves its right to decide whether or not to enter into renewal for the DLP solution after the initial lock in period of 1 (One) year.	DLP Solution Implementation and management is a long-term project and typically all the banks and financial institutions have gone for 5 years contract to realize the benefits of the implemented solution. We request the bank to confirm the contract period for five years.	Please refer to amendment no. 2
21	Page no. 24 Clause no. 1	The DLP Solution should meet the requirements of the Incident Management Process established at Organization, which primarily includes enforcing Organization DLP Policy, end-to-end DLP incident Management, Process Governance, Incident Forensics & On Demand Reporting DLP Solution capability.	Bidder request to share the Incident Management Process, Process Governance model for due-diligence and Solution on boarding purposes.	It is clarified that the details will be provided to the successful Bidder.
22	Page no. 24 Clause no. 2	Discovery, fingerprinting and indexing of Organization Data, classified as per Organization Classification Standard, including but not limited to Organization Customer's PII & SPII & Bank Confidential Data, placed anywhere at network, endpoint systems and web server.	Bidder request to share the Definition criteria for Classified Standards, PII & SPII, Confidential Data to on board the same in Solution proposal document.	It is clarified that these details will be provided to the successful bidder.
23	Page no. 24 Clause no. 3	The DLP Solution should have the ability to identify: · data-in-motion (traveling across the network) · data-in-use (being used at the endpoint). · data-at-rest (sitting idle in storage)	Please clarify more on data in use (being used at the endpoint) Data in motion cannot be achieved fully until we don't have the mail DLP component.	It is clarified that the Data in motion refers to the data flowing through proxy server.
24	Page no. 24 Clause no. 6	The Proposed Solution should capture logs of Data Transfer through any medium like E-Mail, Internet Upload, USB Transfer etc. At the same time intelligently co-relate and analyses these Logs with previous user based attempts / incidents and trigger alerts.	This is a functionality of SIEM to correlate the incidents. The primary role of DLP is to trigger the policy violation based on the parameters that are configured in the policy. Since it is not a functionality of DLP, hence requesting M/s. Indian Bank to consider removing this point.	Please refer to amendment no. 3
25	Page no. 24 Clause no. 7	The proposed solution should be able to discover and identify sensitive information stored on	Currently we don't support SAN & NAS.	Please adhere to RFP Specifications.

		endpoints, databases, file shares, SharePoint, SAN, NAS etc.		
26	Page no. 24 Clause no. 12	Ability to integrate with threat intelligence for enterprises across all locations.	DLP is a solution for data loss; DLP solution will not cover threat intelligence. Threat intelligence comes with the security solutions.	Please refer to the amendment no. 4
27	Page no. 24 Clause no. 13	The Solution should have a capability to capture and index all the traffic flowing out of the Network.	The proposed solution is a DLP technology which captures all contents instead of traffic flow. Hence request to modify this specification as "The solution should have capability to detect the data breach and store the incident for forensic purpose".	Please refer the amendment no. 5
28	Page no. 24 Clause no. 14	The solution should be capable to identify and store data from all TCP Protocols including HTTP, HTTPS, SMTP, FTP.	Kindly confirm whether Bank uses any TLS protocols or not being explicitly not mentioned in the RFP document.	Yes. Bank is using TLS protocols.
29	Page no. 25 Clause no. 15	The proposed solution should have the capability to analyse: • file formats (.doc, .docx, .xls,.xlsx,.ppt,.pptx, .csv, .pdf, .xps etc) • data in archival tools (.zip/.rar/.7z/.tar) • encrypted data over web proxies • data sent over email • attachments of the email	Inspect encrypted data from web proxies. For DLP to read the content, the data has to be decrypted by the proxy and given to DLP. Else, DLP will only detect on the file type and not the content.	Please adhere to RFP Specifications.
			Email attachments can only be Monitored & protected when we will have the Mail DLP component.	Please refer to amendment no. 6
			Please clarify do customer share the decrypted Web traffic from the Proxy solution for DLP inspection.	It is clarified that DLP solution should have Decryption/Encryption capability.
30	Page no. 25 Clause no. 19	The solution should detect and validate a wide range of sensitive data types (e.g., SSNs, CCNs).	SSNs are more relevant to US citizens. Does Bank have the data of US citizens or Defined Business Requirements to implement the same Policy?	It is clarified that SSNs, CCNs are examples. Solution should detect all Data classified by the Bank as sensitive.
31	Page no. 25 Clause no. 20	The Solution should be able to enforce policies to detect data leaks.	This is very generic, but the other specifications have already covered this Point. Hence requesting M/s. Indian Bank to consider removing this point.	Please adhere to RFP specifications.
32	Page no. 25 Clause no. 23	The proposed solution should generate (exception) alerts and reports for contents that could not be decrypted for analysis as part of DLP solution.	Please Elaborate.	Please refer to amendment no. 7
			We need clarify on this specification as we detect the encrypted files and alert the admins. Also we request	

			M/s. Indian Bank to modify the specification as "The proposed solution should be able to detect the encrypted files and trigger incidents".	
33	Page no. 25 Clause no. 32	The Solution should have out of the Box rule sets or PII Policy templates.	Kindly requesting M/s. Indian Bank to remove this point because it is already covered in another specification.	Please adhere to RFP specifications.
34	Page no. 25 Clause no. 34	The Proposed Solution should be able to perform following Searches: * E-Mail Sent from or to any E-Mail Address.	Need more clarity on what is expected in the search. This is a DLP solution which generates incidents based on content and captures required fields. Email attachments can only be Monitored & protected when we will have the Mail DLP component.	Please refer to amendment no. 8
35	Page no. 26 Clause no. 34	The proposed solution should be able to perform following searches * Traffic sent across protocols or ports. * Documents leaving the network based on Document Type * Filename and Timestamp	DLP works on Web (http, https & FTP), Email and Endpoint Channels. All these achieved by doing integration methods on various channels. So, requesting M/s. Indian Bank to remove this point as the channels have been covered the specification already.	Please adhere to RFP specifications.
36	Page no. 26 Clause no. 35	In case of Policy violation the solution should be able to retain all content/attachments in the transaction, not just the content that violated policy.	DLP will retain the attachment which violated the policy and show in the incident. Not all attachments. Need to clarify this.	It is clarified that the solution should capture all attachments which violated the policy.
37	Page no. 26 Clause no. 41	The solution should have ability to detect cumulative malware information leaks. The solution should be able to detect data leaks over to competitors and the data sent and uploaded after the office hours predefined patterns. The solution should also be capable of detecting and blocking the sensitive information uploads to Group of P2P software i.e. Bit Torrent, eMule etc.	DLP is a solution for data loss; DLP solution will not cover malware information leaks. Detecting data leaks over to competitors and the data sent and uploaded after the office hours predefined patterns will not be covered with data loss as it depends on the User Behaviour. Not a data loss prevention use cases, it will be a proxy based solution.	Please refer to amendment no. 9
38	Page no. 26 Clause no. 43	The proposed Data Protection solution should be able to address the following key area:	The DLP works on policies to identify the content using various technologies; those have been covered in the specification already. So requesting M/s. Indian Bank to remove the 1st point.	Please adhere to RFP specifications.

		• Identify data leakage across all vectors, irrespective of policy being in place or not • Discover and Protect Sensitive data • Have flexible control over Remediation of Data Leakage • Ease of Use and Quick to Deploy • Educate the users and the management so as to reduce the risk	Detection will happen only based on defined policy. Please clarify on the 1st point " Identify data leakage across all vectors, irrespective of policy being in place or not.	It is clarified that solution should be able to detect Data leak by its standard policy even though customised policies are not being placed.
39	Page no. 26 Clause no. 44	The Solution should Index all unfiltered files during discovery process.	The DLP solution works based on content, so request you to modify this point as " The solution should discover the files based on DLP policies and help to remediate the violations"	Please adhere to RFP specifications.
40	Page no. 26 Clause no. 45	The solution should allow export historical records from all traffic / content analysed by DLP system into an external system for Analysis.	This is a duplicate point as the SIEM integration specification is already mentioned in the RFP. So please remove this specification.	Please adhere to RFP specifications. It is clarified that one of external system is SIEM tool.
41	Page no. 26 Clause no. 46	The Solution should be able to classify the data as content based, context based and user based.	DLP is not a classification technology, hence requesting M/s. Indian Bank to remove this point. In the other specifications where it is mentioned about the integration with classification tools, IRMs.	It is clarified that the solution proposed should have data classification technology.
42	Page no. 26 Clause no. 47	The proposed solution should provide SSL decryption and destination awareness capability on the gateway to identify any sensitive content uploading to online web properties, even when it is tunnel over SSL.	Capability of looking the in to encrypted traffics on network requires a ICAP integration. This can be achieved by the doing the ICAP integration with the existing proxy solution or do we need to consider this as well.	Bank currently have proxy servers which requires ICAP integration.The successful bidder has to provide and implement necessary hardware and software to meet the requirement.
			SSL protocol is fully vulnerable to multiple exploitations. Does bank still use the same?	It is clarified that the tunnelling protocol used for accessing the content on web depends on the provider. Bank is using TLS1.2

				The term SSL in the specification includes all its upward revisions. Please adhere to the RFP specifications.
43	Page no. 26 Clause no. 50	The solution should support scanning of database such as Oracle, Microsoft SQL Server, My SQL and IBM DB2.	Currently we don't support IBM DB2.	Please adhere to RFP Specifications.
44	Page no. 27 Clause no. 52	The solution must manage all DLP security products (e.g., software, appliances) from one centralized administration console, even encryption of files and folders.	This is DLP specification. The file and folder encryption is a different technology, hence requesting M/s. Indian Bank to remove this point.	Please refer to amendment no. 10
45	Page no. 27 Clause no. 54	The proposed solution should be able to integrate with Office365 and its mail DLP policies.	Integration of DLP policies on office 365 can be performed with the Outlook application on the endpoints. But comprehensive solution of Office 365 would be a CASB solution as we have to look at unmanaged device and users accessing it from corporate or non-corporate device accessing the data.	Please adhere to RFP Specifications.
46	Page no. 27 Clause no. 55	The solution should allow creation of custom patterns and the vendor should also create custom patterns based on the banks needs without any additional cost.	We need clarify on this specification as we detect the encrypted files and alert the admins. Also we request M/s. Indian Bank to modify the specification as "The proposed solution should be able to detect the encrypted files and trigger incidents. This is also a duplicate statement as same is mentioned in the specification.	Please adhere to RFP specifications.
47	Page no. 27 Clause no. 58	The Proposed solution should comply with PCI DSS requirements.	The PCI DSS has various requirements not only limited to data protection. Since this RFP is specific to data protection, kindly modify the specification as "The proposed solution should help the bank to enforce controls to protect credit / debit cards".	It is clarified that PCI DSS requirements related to DLP should be complied.
48	Page no. 27 Clause no. 60	The solution should be able to detect sensitive data going out in the form of all different images formats.	There are two same points, so kindly requesting M/s. Indian Bank to remove any one of the above specifications.	Please refer to amendment no. 11
49	Page no. 27 Clause no. 62	The solution should not be based on only file extension to determine content type, instead offered solution uses signatures, statistical analysis,	Need more clarification. Context based detection for file type is via file extension.	It is clarified that solution should be able to inspect the content of the file

		lexicons, and other techniques to detect the content type based on its structure and data.		irrespective of file extension. (i.e. user changing .exe file to .zip)
50	Page no. 27 Clause no. 64	The solution should be able to enforce policies to detect data leaks even in image files through Optical Character Recognition technology. It should support file formats like .jpeg, .png, scanned .pdf and other commonly used formats.	Currently we support only Image files & PDF files. Both are same points, so kindly requesting M/s. Indian Bank to remove any one of the above specifications	Please adhere to RFP Specifications.
51	Page no. 27 Clause no. 71	The proposed solution should support 256 bit or higher encryption for transfer of information.	Is this for DLP components communication?	It is clarified that the specification is for communication between management console and backend servers used for DLP solution.
52	Page no. 28 Clause no. 74	The solution should be scalable as per Banks future requirements.	This is very generic, we need to understand in terms of what changes or expansion come on infrastructure, so it helps us to design the solution appropriately	It is clarified that the solution should be scalable up to 30,000 endpoint and web users.
53	Page no. 28 Clause no. 76	The proposed solutions should maintain the audit trail for the management activities of individual users and administrators accessing and using the application.	Two specifications are same in functionality, so kindly remove one of the specifications.	Please adhere to RFP Specifications.
54	Page no. 28 Clause no. 78	The proposed solution should have audit control to track the changes done in policies.	Two specifications are same in functionality, so kindly remove one of the specifications.	Please adhere to RFP Specifications.
55	Page no. 28 Clause no. 2	The solution should be IPv6 compatible. The bidder should assist the bank in migration to IPv6 as and when the bank decides to migrate to IPv6 for devices in scope.	We don't Support IPV6 Currently and have a road map in the upcoming versions.	Please adhere to RFP Specifications.
56	Page no. 29 Clause no. 12.2	One management server at DC and one at DR Site to be proposed for the management of servers and configuring policies.	We can deploy the management server at one location Bidder recommends to have minimum 02 Servers in each category for DC and 01 Server in each category for DR to achieve the 99.5% availability SLA unless it won't be able to achieve with non HA configurations.	Please adhere to RFP Specifications.

57	Page no. 29 Clause no. 12.3	The Successful bidder should provide onsite support at Chennai.	Please clarify that How many engineers are required at Chennai? Are the resources to be deputed 24*7 or 10:00 to 6:00 PM? Is this onsite engineer is required during the project phase or the entire contract period of 5 years.	It is clarified that On-site engineer is required till project Sign-off.
58	Page no. 30 Clause no. 13.9	In case Bank decides for relocation of Servers, Upgrade the existing Servers, purchase new Servers with higher end configurations, appropriate support should be provided for installation, reinstallation, upgrading, etc., based on the Bank's requirements and the successful bidder should ensure that the proposed Services/Solutions are continuously made available across the Bank's network seamlessly.	What will be the probability of the relocation in a period of one year?	Nil
59	Page no. 31 Clause no. 2	Minimum annual turnover of Rs.60.00 Crores during each year out of which at least Rs.20.00 Crores should be from the information security domain.	Please note we do not report financials product wise, hence the requested turnover from security domain is not possible to report. Request you to change this to Bidder/OEM should have minimum annual turnover of Rs.60.00 Crores. Request bank to change the clause to average turnover of Rs.60 Crores in last 3 financial years.	Please adhere to the terms and conditions of RFP.
60	Page no. 31 Clause no. 2	Bidder should be profit making company during the last 3 consecutive financial years of the bidder (2015-16, 2016-17 and 2017-18).	Bidder should have earned Net/Operating profit for last 2 years (FY 17-18 & 16-17) (or) The bidder or its parent company (bidder should be 100% owned subsidiary of the parent company) has registered net profit for at least two financial years (Financial year shall mean an accounting period of 12 months.	Please adhere to the terms and conditions of RFP.
61	Page no. 31 Clause no. 3	The Bidder should be in the business of providing/handling Information Security Solutions/ Services/Management since at least last 5 years as on 31.12.2018.	Request Bank to Change the clause to at least 1 year as on 31.12.2018.	Please adhere to the terms and conditions of RFP.
62	Page no. 31 Clause no. 4	The Bidder should have Support Centres in Chennai, Hyderabad, Mumbai, New-Delhi & Kolkata.	Support centres in all locations – We assume the scope is only one time implementation of the proposed solution and no need to manage on-going basis which Bank will take care. Please elaborate the scope of the bidder on Post sale support required.	It is clarified that On-call support is required post sales.

इंडियन बैंक / INDIAN BANK
कॉ.का / C.O.
आईटीडी / ITD
चेन्नै / CHENNAI-600 014

			Please give relaxation for Kolkata location alone.	Please adhere to the terms and conditions of RFP.
63	Page no. 31 Clause no. 5	Bidder should be ISO 27001 certified.	Request to remove the clause and replace with ISO 9001 certified.	Please adhere to the terms and conditions of RFP.
64	Page no. 31 Clause no. 6	The bidder should have highest level of partnership with OEMs of the product quoted in the bid. The Bidder must be in position to provide support / maintenance / upgrade of the Solutions during the period of contract with the Bank.	The criteria for giving the partnership status by OEM mainly depends on the Volume of Business the partner does for a particular OEM ,we request the bank to change this criteria to "The bidder should have highest level/at least 2 levels below the highest level of partnership/ Certified engineers on products proposed with OEMs in the bid. The Bidder must be in position to provide support / maintenance / upgrade of the Solutions during the period of contract with the Bank.". Bank can also ask for minimum number of certified Engineers for the proposed solution to be one of the criteria for judging the bidders capability.	Please adhere to RFP terms and conditions.
65	Page no. 31 Clause no. 7	The bidder should be a System Integrator for the Security Solutions quoted and should have successfully implemented the Solutions at a minimum of one Bank/Financial Institutions/Public sector enterprises/ Govt. Organizations in India during the last three years (31.12.2018).	Bidder should have successfully implemented the Solutions at a minimum of one Bank/Financial Institutions/Public or Private sector enterprises/ Govt. Organizations in India during the last three years. Request the bank to modify this to last 5 years. Request the bank to modify this to last 7 years.	Please adhere to the terms and conditions of RFP.
66	Page no. 31 Clause no. 9	The DLP solution quoted should be in Gartner Quadrant for DLP.	Request to Include all Quadrant of Gartner for consideration.	Please adhere to the terms and conditions of RFP.
67	Page no. 19 Clause no. 16.c	Termination by Default.	Please confirm that such costs or damages shall be as per any court award or damages determined by competent authority only.	Please adhere to terms and condition of RFP.
68	Page no. 13 Clause no. 3	Performance Security.	Please clarify that the performance security shall be invoked by the Bank only in case of a material breach by the bidder. Also, the material ground of contract signing shall be only on the basis of mutual agreement.	Please adhere to terms and condition of RFP. However Bank will inform successful bidder that the Bank guarantee invoked for non-

				performance in writing before going for invoking the performance security.
69	Page no. 15 Clause no. 7	Warranty.	Bidder confirms that all goods delivered are subject to the warranties provided by the OEM. Please note that insofar as is legally and contractually permissible, Bidder will pass onto, resell, or assign to Bank all the third party warranties. Kindly acknowledge and confirm this understanding.	Please adhere to terms and condition of RFP.
70	Page no. 19 Clause no. 15	Termination for convenience.	Termination for convenience must be subject to 90 days written notice. Further, all dues outstanding to bidder along with a pre-determined termination fees shall be cleared within 30 days of such termination.	Please adhere to terms and condition of RFP.
71	Page no. 19 Clause no. 16	Termination for default.	Please incorporate a notice period of 30 days at least so that bidder may rectify any defaults during such time.	Please adhere to terms and condition of RFP.
72	Page no. 21 Clause no. 23	Limitation of Liability.	Please add this to the limitation of liability clause: Bidder's aggregate liability under the contract shall be limited to a maximum of 10% of the contract value per year. Neither party shall, in any event, regardless of the form of claim, be liable for any indirect, special, punitive, exemplary, speculative or consequential loss or damages.	Please adhere to terms and condition of RFP.
73			Number of proxy solutions in the network and locations?	Currently Bank is having Web proxy of different OEMs. It is clarified that exact nos. and location will be provided to the successful bidder.
74			Any mobile devices along with the Endpoints like smartphones, tablets etc.?	No.
75			Minimum Hardware requirements were provided in the RFP, what in case solution comes with the prebuilt hardware?	It is clarified that the bidder should provide the hardware and software required for implementation of solution at DC and DR Site.

76			Throughput of the network?	Bank Network Devices are connected using 1Gbps Links.
77			We request the Bank to provide the details: 1) Tools used for deploying the patches/updates (Ex:SCCM) 2) OS flavours(Windows/MAC) which are running at Endpoints/Servers 3) The list of Web Applications/Endpoint Applications. 4) The Browsers running on the Endpoints. 5) The AV used at Endpoints/Servers. 6) Details of identity Store (AD/LDAP) 7) Tool which is used Data Classification and Data Flow 8) License and versions available for Windows /SQL which can be used for deployment 9) Data Retention policies to size the Hardware accordingly. 10) Number of users who will be roaming (Laptops).	It is clarified that Data required for implementation of DLP solution will be provided to the successful Bidder.
78			Does bank implemented Data Classification solutions? Please provide details to check the compatibility.	No. Data Classification solution should be provided as a part of this project.
79			Difference in Web DLP license (11K) and Endpoint DLP license (21K)?	It is clarified that all user endpoint users are not using Web proxies. Hence the difference in user.
80			Will bank allow to push the endpoints using customer Patch Management Solution to all endpoints across all sites?	It is clarified that the successful bidder is permitted to use systems in the bank to push the DLP agent software to endpoints
81		Clause not present in RFP	Wipro's failure to perform its contractual responsibilities, to perform the services, or to meet agreed service levels shall be excused if and to the extent Wipro performance is affected, delayed or causes non-performance due to Customer's omissions or actions whatsoever.	It is clarified that if the successful bidder is unable to meet the contractual responsibilities, to perform the services, or to meet agreed service levels due to reasons attributable to the

				Bank, The successful bidder should inform the Bank that deliverables could not be met due to reason listed and Bank should accept the reasons.
82		Clause not present in RFP	Services and/or deliverables shall be deemed to be fully and finally accepted by Customer in the event when Customer has not submitted its acceptance or rejection response in writing to Wipro within 15 days from the date of installation/commissioning or when Customer uses the Deliverable in its business, whichever occurs earlier. Parties agree that Wipro shall have 15 days' time to correct in case of any rejection by Customer.	Accepted.
83		Clause not present in RFP	Customer hereby agrees to make the site ready as per the agreed specifications, within the agreed timelines. Customer agrees that Wipro shall not be in any manner be liable for any delay arising out of Customer's failure to make the site ready within the stipulated period, including but not limited to levy of liquidated damages for any delay in performance of Services under the terms of this Agreement. In case the SITE is not ready for a continuous period of 30 days, milestone payment related to installation will be released to vendor based on the SNR report, also if there is any additional warranty cost due to continuous site not readiness for 30 days, same will be borne by the customer.	It is clarified that the Site is ready.
84		Clause not present in RFP	Since Wipro is acting as a reseller of completed products, Wipro shall "pass-through" any and all warranties and indemnities received from the manufacturer or licensor of the products and, to the extent, granted by such manufacturer or licensor, the Customer shall be the beneficiary of such manufacturer's or licensor's warranties and indemnities. Further, it is clarified that Wipro shall not provide any additional warranties and indemnities with respect such products.	Please adhere the terms and conditions of RFP.

85			Need clarity on the type of support requested in branch location for troubleshooting. Since only endpoint agent is proposed at the remote branch locations. We assume no visit required for remote branch locations.	It is clarified that telephonic support is required for implementation and operations at branches. However in exceptional cases where solution is not working or solution is hindering day-to-day operations of the branch, Visit of engineer to branch is required.
86			Please share the details of the existing Email Security Gateway and Proxy Solution for checking integration compatibility. Also require location details where the existing Proxy and Email security solutions are available.	It is clarified that the information sought is classified in nature and cannot be published in open.
87			Please confirm bank is having the NMS and Infra monitoring tool to monitor the DLP hardware assets availability and performance.	Yes.
88			Tata communications assumes the bank is having well defined data classification policies with good amount of user awareness and adherence.	It is clarified that the Bank existing polices and other details required for the project will be provided to the successful bidder.
89			Please confirm the bank has identified the information assets where the critical data is residing, and the data classification mechanism is in place already.	Yes.
90			We request banks to provide information on existing Service Desk tool with which the DLP solution to be integrated for ITIL process adherence.	It is clarified that details will be provided to the successful bidder.
91			a. We request banks to provide information on existing SIEM tool with which the DLP solution to be integrated for Incident identification and severity categorisation. b. Banks's SOC team will do the incident monitoring and raise the tickets on service desk tool through which DLP	a. It is clarified that details of existing SIEM solution will be provided to the successful bidder.

			service provider will act upon the incidents. Please confirm.	b. Yes.
92			We assume that the DLP use cases for SIEM to be provided by Bidder and Bank's SOC team will develop on the SIEM platform.	Yes.
93			Do we have incident/Change severity levels defined with response and resolution times?	Yes.
94			We assume Bank will provide the role-based access to the service desk and SIEM tool. Please confirm.	Yes.
95			There will be at least 1000s of events / incidents / logs on frequent basis. Helpdesk Services for managing the DLP solution post implementation has not been mentioned in the RFP. Please Clarify who will manage the same.	Post sign-off, the solution will be managed by the Bank including daily operations.
96			System requirements for DLP including Enforce Server, Oracle Database Server, Web Prevent & Network monitor. Please clarify whether this can be provisioned from your existing Virtualisation layer.	Bidder has to provide all necessary Hardware and software required for the implementation and operation for the contract period.
97			Bank has to ensure to take up the responsibility of providing 21000 systems and resolve any issues preventing the System Integrator from deploying the DLP solution to the 21000 endpoints.	It is clarified that the Bank will provide details of systems for implementation of DLP solution for the licenses procured.
98			Bank has to ensure & confirm the System Integrator to make use of the existing software deployment solutions present at the bank to roll out DLP client software. Bank need to Co-ordinate between System Integrator and Software deployment solution team to ensure DLP client is rolled out to all systems.	It is clarified that the successful bidder is permitted to use systems in the bank to push the DLP agent software to endpoints.